

ABSTRACT

A method to enable dynamic configuration of gaming terminals installed in one or a plurality of gaming premises whereby certified games, certified data files and certified support software components are activated in accordance with a predetermined schedule or automatically in response to the observed gaming activity. The method may include allocating an individual PKI certificate to each executable software component and each of its versions, binding the PKI certificate to the executable software, associating a distinctive policy for each certificate and then enforcing the software execution policies in accordance with the desired authorized game configuration and schedule. The PKI certificate's "Subject Name" (or "Issued to" field or "CommonName" field) may be a concatenation of the software component identification, its version number and optionally other identification characters. The method applies equally to other network connected gaming subsystems. The method enables a fine-grained and secure control of the authorized software components and thus the flexibility to securely configure the gaming system in accordance with a schedule or in a close-loop fashion in order to meet business objectives. In addition, a method to enable the certification authority to bind the certificates to the tested code is described.